ESA GPT - Auftragsbearbeitung nach Art. 9 DSG

Die ESA - Einkaufsorganisation des Schweizerischen Auto- und Motorfahrzeuggewerbes Genossenschaft (nachfolgend AN) stellt dem Auftraggeber (nachfolgend AG) die Dienstleistung ESA GPT zur Verfügung, welche auch die Bearbeitung von Personendaten umfasst und eine Auftragsbearbeitung im Sinne von Art. 9 DSG darstellt. Für die Nutzung von ESA GPT gilt diese Auftragsbearbeitungsvereinbarung (ABV) formlos. Version 1.0 vom 28.04.2025, diese Version kann durch zukünftige Versionen ersetzt werden.

Kategorien Betroffener:	Kunden, Mitarbeitende, Geschäftspartner des AG
Datenkategorien:	Kontaktdaten, Nutzungsdaten und vom AG bereitgestellte Daten
Zulässiger Datentransfer (Land):	Daten werden in der CH und im EWR (DE, IRE, SWE) bearbeitet

Genehmigte Unterauftragsbearbeiter (Name, Zweck): Microsoft Ireland Operations, Hosting von Azure OpenAI (CH und SWE) und Statworx GmbH, Implementierungspartner (DE)

Pflichten des Auftragnehmers (AN)

1. Der AN bearbeitet Daten nur für Zwecke und nur auf dokumentierte Weisung des AG (z.B. Bereitstellung KI-Umgebung); hält er sie für unzulässig, sagt er dies dem AG.

2. Der AN sorgt stets für eine angemessene Datensicherheit gemäss geltendem Datenschutzrecht und gemäss den TOM. Jede Verletzung der Datensicherheit meldet er ohne Verzug mit allen Infos.

3. Der AN verpflichtet alle Hilfspersonen und Mitarbeiter zur Geheimhaltung, soweit sie dies nicht schon von Gesetzes wegen sind.

4. Der AN nutzt Unterauftragsbearbeiter nur mit Genehmigung (s.o.). Über weitere muss informiert werden und sie gelten ohne Widerspruch innert 30 Tagen als genehmigt. Diese sind ebenso zum Datenschutz zu verpflichten.

5. Der AN exportiert keine Daten des AG ohne dessen Erlaubnis und wenn, dann nur unter Befolgung des geltenden Datenschutzrechts.

6. Der AN unterstützt den AG bei Bedarf bei der Einhaltung des Datenschutzrechts, insb. zur Erfüllung von Betroffenenrechten und bei Datenschutz-Folgenabschätzungen.

7. Nach Ende der Zusammenarbeit werden die Daten nach Ablauf der gesetzlichen Aufbewahrungsfristen vernichtet.

8. Der AN weist die Einhaltung dieses ABV nach und der AG kann dies überprüfen.

Informationssicherheit (TOM)

Nachfolgend unsere technischen und organisatorischen Massnahmen (TOM) zur Datensicherheit.

- Zutritts- und Zugangskontrollen
- Videoüberwachung Warenlager und Serverraum
- USV
- IAM
- Datenzugriffe nur mit Authentifizierung
- MFA für alle Zugriffe
- Starke Passwörter
- Least-Privilege-Prinzip
- Need-to-know-Prinzip

- Zero-Trust-Prinzip
- Endgeräte verschl.
- TLS enforced
- Penetration Tests
- ext. Security Audits
- ISMS
- Backups
- BCM-Konzept
- Firewalls
- IDS
- EDR/XDR
- MDM
- Malwareschutz
- Patchmanagement
- Trennung produktive/andere Systeme
- Installation von Software kontrolliert
- SOC
- Weisung Informationssicherheit
- Security Awareness Trainings
- Protokollierung sicherheitsrelevanter Ereignisse.

detaillierte TOM auf Anfrage erhältlich